CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** December 16th, 2025 - January 6th, 2026
Distribution: Public Sector Partners, Local Governments, IT Departments *Volume 2 Issue 1*

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Windows 10/11 Zero-Day Exploit	General	An actively exploited Zero-Day that allows threat actors to engage in privilege escalation vulnerability in the Windows Cloud Files Mini Filter Driver.	According to Microsoft, the vulnerability has been patched as of the Windows Patch on Tuesday, December 9, 2025. All users need to patch vulnerability in order to update their Operating System.
Fortinet Inc. Exploits	Technology Infrastructure	An improper verification of cryptographic signature for data a handful of Fortinet's applications. This allows unauthenticated users to bypass the FortiCloud SSO login via a crafted SAML message.	To prevent affected versions from being exploited, FortiGuard Labs suggests temporarily disabling FortiCloud login until the system can be upgraded to a non-affected version. All non-affected versions are available on FortiGuard's website.
CISA's Industrial Control Systems Advisories	Public Infrastructure, Education, Healthcare	ICS advisories were given to address cybersecurity vulnerabilities in a wide range of industrial, building management, security, energy, healthcare, and automation systems.	CISA recommends that organizations review each advisory in detail, apply available patches or updates, and implement mitigations to minimize damage issues with no current available patches.
CISA's Top 25 Most Dangerous Software Weaknesses	All Sectors	In collaboration with MITRE, CISA released a list of the 25 most critical software weaknesses commonly exploited by adversaries.	Enforce automated security testing and continuously track CWE-mapped weaknesses to reduce risk. Implement rigorous input validation, robust authentication, and authorization controls.
AI Development Tooling Risk	General	A command injection flaw in the GitHub Copilot plugin. This can lead to arbitrary code execution on the affected system without privileges or user interaction.	Update the GitHub Copilot plugin for JetBrains to version 1.5.60-243 or later.

CERIAC
Cybersecurity Education, Research and Outreach Center

Important Government and ISAC Alerts

- **CISA ICS Advisories:** CISA Releases Six Industrial Control System Advisories
  Vulnerabilities impacting industrial, building management, energy, healthcare, automation, and security systems across public infrastructure, education, and healthcare environments - risks include unpatched flaws that may allow system compromise.
- **CISA ICS Medical Advisory:** Varex Imaging Panoramic Dental Imaging Software
  Vulnerability affecting healthcare imaging systems used in dental environments that could be exploited to allow local privilege escalation.

Security Awareness Theme

December Focus: **Public Wi-Fi Networks**

Public Wi-Fi Networks that are usually found in cafes, airports, hotels, and even malls are usually convenient but often unsecured. This is because they usually lack strong encryption, making available for attackers to intercept data or trick user into connecting to malicious network.

Train yourself to **pause and inspect** before joining an open network.

Common Red Flags:

- Networks with **no password** required or **vague names (“Free_ Wifi”)**
- Duplicate Wi-Fi names with slight spelling differences
- Unexpected login pop-ups or security warnings
- HTTPS missing from websites
- Requests to install certificates or software

Action Tips to Stay Safe:

- Avoid logging into sensitive accounts (Email, Bank, etc)
- Disable auto-connect to open Wi-Fi networks
- Only visit websites with HTTPS
- Keep devices updated with security patches

Sector-Specific Highlights

- **Healthcare:** WHILLS Model C2 Electric Wheelchairs and Model F Power Chairs - On these models of WHILLS wheelchairs, no authentication was required for Bluetooth connection. This allowed attackers to bypass direction commands and speed controls on these wheelchairs. ***Prevention Tips:*** *Remove internet connection from these devices.*

- **Utilities/Industrial:** Operation "BRICKSTORM" - The People's Republic of China has positioned malicious software in critical infrastructure devices across the United States within the industrial sector. This software is designed to "brick" or completely disable the infected device. ***Prevention Tips:*** *Use IOCs and detection signatures to identify "BRICKSTORM"* data signatures.

- **Education:** University of Phoenix Data Breach – A group going by the name of Cl0p has targeted several colleges across the U.S., most recently targeting University of Phoenix through an Oracle E-Business Suite vulnerability. ***Prevention Tips:*** *Any school using the Oracle E-Business Suite should update past 12.2.14.*

- **Public Safety/Financial:** "Sturnus" - "Sturnus" is an Android trojanware that can bypass common security measures, including chat encryption, to surveil users. It can also create banking login screens to phish credentials with high accuracy. ***Prevention Tips:*** *Be cautious when downloading APKs on Android devices from other providers besides the Google Play Store. Google released a statement recently, reporting that there were no instances of "Sturnus" published on it's platform.*

Recommended Tools and Federal Resources

- MS-ISAC – A free resource suite to help state and local governments build cybersecurity awareness and education programs.
- Research Security Training – The National Science Foundation provides online research security training geared toward academic research.
- CISA's Online Toolkit to Safeguard K-12 – Education sector focused resource that provides self-paced online courses for the fundamentals of Cybersecurity.

Emerging Trends to Watch

- OS Command Injection – The application executes a single, fixed program that is intended to use externally-supplied inputs as arguments to that program. It can also accept an input that it uses to fully select which program to run, as well as which commands to use. ***Prevention Tips:*** *If possible, use library calls rather than external processes to recreate the desired functionality.*

- Deserialization of Untrusted Data – Attackers can modify unexpected objects or data that was assumed to be safe from modification. Deserialized data or code could be modified using the provided accessor functions, or unexpected functions could be invoked. ***Prevention Tips:*** *If available, use the signing/sealing features of the programming language to assure that deserialized data has not been tainted. When deserializing data, populate a new object rather than just deserializing.*

- Path Traversal - Attackers can overwrite or create critical files, such as programs, libraries, or important data. This may prevent the product from working at all and in the case of protection mechanisms such as authentication, it has the potential to lock out product users. ***Prevention Tips:*** *Implement input validation that assumes all input is malicious. Use an "accept known good" validation strategy and reject any input that does not strictly conform to specification or transform it into something that does.*